iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** III **Month of publication:** March 2022

DOI: https://doi.org/10.22214/ijraset.2022.40854

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue III Mar 2022- Available at www.ijraset.com

User Activity Monitoring System /SPYWARE

Ms. Sakshi Sanklecha[1], Mr. Darshit Deotale[2], Ms. Jyoti Yadav[3], Ms. Dipti Mishra[4], Prof V. P. Yadav[5]
[1, 2, 3, 4, 5]*Research Scholar,* [6]*Assistant Professor, Department of Computer Science and Engineering, Priyadarshini College of Engineering, Nagpur, India*

Abstract: ***User activity monitoring (UAM) do the task of monitoring and recording of user actions, in the field of information security or cyber security. Including the use of applications, windows opened, system commands executed, checkboxes clicked, text entered/edited, URLs visited and nearly every everything on-screen event to protect data by ensuring that employees and contractors are performing their assigned tasks and not posing any risk to the organization are all captured and recorded in the system by the UAMS. Video-like playback of user activity and process the videos into user activity logs that keep step-by-step records of user actions that can be searched and analysed is delivered by the User Activity Monitoring System to investigate any out-of-scope activities. Creating a visual record of potentially hazardous user activity are all involved in Visual Forensics. Each user action is logged, and recorded.***
Once a user session is completed, UAM creates a written record as well as visual record. It can be screen- captures/screenshots or video of exactly what kind of activity a user has done. This written record of our UAMS differs from that of a SIEM or logging tool, because it captures data at a user-level not at a system level –providing plain English logs rather than System Logs (which is originally created for debugging purposes).
These textual logs can be used to pair with the corresponding screen- captures/screenshots or video summaries. Using these corresponding logs and images, the visual forensics component of UAM allows for organizations to search for exact user activity in case of a security incident. In the case of a security threat, i.e. a data breach or data leak, visual Forensics are used to show exactly what kind of activity a user has done, and everything leading to the incident. Visual Forensics can also be used to provide evidence to any law enforcement that investigate the intrusion or leak.

I. INTRODUCTION

Tools that monitor and track end user behaviour on devices, networks, and other company-owned IT resources are nothing but the Activity Monitoring Systems. UAMS help us to detect and stop insider threats, whether unintentional or with malicious intent that's why it is in use by many organizations . Methods utilization and monitoring are all depends on the objectives of the company. For more readily identifying of suspicious behaviour and heavy risks before they result in security violations, or at least in time to minimize damages such type of softwares are implemented. Sometimes called user activity tracking, user activity monitoring serves as a proactive review of end user activity to determine misuse of access privileges or data protection policies either through ignorance or malicious intent but is a form of surveillance. Protecting information while ensuring availability and compliance with data privacy and security regulations all are the purpose of user activity monitoring. UAM goes beyond simply monitoring network activity. All types of user activity, including all system, data, application, and network actions that users take are all monitored. Web browsing activity of user, whether users are accessing unauthorized or sensitive files, and more are all the examples that UAMS can monitor.

There are various methods implemented to monitor and manage user activity such as:

A. File/Screenshot Capturing

After every 0.2 sec capturing of scrren goes on continuously until it has been stop by the server

B. Log collection and Analysis

It is the process of reviewing, interpreting and understand computer-generated records called logs. Logs are generated by a range of programmable technologies, including networking devices, operating systems, applications, and more. Log analysis involves collecting, evaluating, and managing the data reported by various components. It is the practice of managing all of the log data produced by your applications and infrastructure

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue III Mar 2022- Available at www.ijraset.com

C. Network packet Inspection

It refers to the method of examining the full content of data packets as they traverse a monitored network checkpoint. With normal types of stateful packet inspection, the device only checks the information in the packet's header, like the destination Internet Protocol (IP) address, source IP address, and port number. DPI examines a larger range of metadata and data connected with each packet the device interfaces with.

D. Keystroke Logging

The process used to view or record both the keystrokes entered by a computer user and the computer's response during an interactive session. These are used to quietly monitor your computer activity while you use your devices as normal. Companies have the legal ability to use key-logger software on business computers, deploy video surveillance cameras, monitor worker attentiveness, track physical movements through geolocation software, compile lists of visited websites and applications, monitor emails, social media posts, and collaboration tools.

E. Kernel Monitoring

Kernel probes are a set of tools to collect Linux kernel debugging and performance information. Developers and system administrators usually use them either to debug the kernel, or to find system performance bottlenecks. The reported data can then be used to tune the systemfor better performance.

All of the information gathered must be looked at within the boundaries of company policy and the user role to figure out if inappropriate activity is in play. What constitutes “inappropriate user activity” is up to the company deploying the UAM solution, and can include anything from visiting personal sites or shopping during work hours to theft of sensitive company data such as intellectual property or financial information.

Manuscript received on January
Revised Manuscript received on January
Manuscript published on January
Sakshi Sanklecha, Student, Dept. of CSE, Priyadarshini College of Engineering, Nagpur, India. Email:-sakshisanklecha12@gmail.com
Darshit Deotale, Student, Dept. of CSE, Priyadarshini College of Engineering, Nagpur, India. Email: j067159 @gmail.com
Jyoti Yadav, Student, Dept. of CSE, Priyadarshini College of Engineering, Nagpur, India. Email: jyotivinodyadav65@gmail.com
Dipti Mishra, Student, Dept. of CSE, Priyadarshini College of Engineering, Nagpur, India. Email: diptimishra200017@gmail.com
Virendra Yadav, Assistant Professor, Dept. of CSE, Priyadarshini College of Engineering, Nagpur, India

Spyware is software with malicious behaviour that aims to gather information about a person or organization and send it to another entity in a way that harms the user. For example, by violating their privacy or endangering their device's security. This behaviour may be present in malware as well as in legitimate software. Websites may engage in spyware behaviours like web tracking. Hardware devices may also be affected. Spyware is frequently associated with advertising and involves many of the same issues. Because these behaviours are so common, and can have non-harmful uses, providing a precise definition of spyware is a difficult task.

II. REVIEW OF LITERATURE

Literature Review Today's Lab Assist. has to take care of all the PC’s all alone. And has to keep an eye on each and every student while they are performing practical’s whether they are really doing assigned work or doing some suspicious activity. And it is extremely difficult to keep an eye on each PC at the same time. To overcome this problem, we develop an online application for the Java programming language. Java is perfectly acceptable and workable for web development and actualy better than .net and Python. Java is a general Programming language.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue III Mar 2022- Available at www.ijraset.com

It is an Object Oriented, static type language. Fromhis experience if we use the right web development tool then java is definitely a great language for web development. Java is perfectly fine for small websites, you can get JSP pages working very quickly with a Java Web Server such as Tomcat. The main reason for large companies choosing Java over other solutions is because it is considered to be much more secure.

A. Features of Java

1) Java is a truly platform independent programming language that supports many operating systems as well as types of hardware.
2) Java is a highly scalable programming language.
3) Java is an open source language, which means it is available free of cost.

Now-a-days, in this 21st century era of computer generation, viewing in the sense of updated technology Lab assists take care of all the PC's alone. It gets extremely difficult to keep an eye on each PC at the same time. It also gets difficult to keep an eye on users about suspicious activity the user is doing in offices on the PCs connected on the same network. To overcome this problem, we are developing this online application by using Java Programming Language. It is Object oriented and static type language. Easy to get JSP working very quickly and in a secure ways.

III. RESEARCH METHODOLOGY

In this study, each client will be given some task, they have to complete the task on time. To have the monitoring on their work, we are developing this system. If any suspicious task is given to the client and client is sending that precious data to other person it can also be caught easily. If any crime occurs during the worktime then also for catching the person who has done the crime the system will be helpful. At many places like departmental works the system can be use because the client sitting on the client-side PC will not know the system is getting monitored. All the monitored data will be stored in the server-side PC's database where the location is provided.

There are mainly two modules :-

1) Spy-server
2) Spy-client.

Spy-server and all PC's of Spy-client should be connected in same network for monitoring. Firstly, we have to init the thread of spy-client and run the spy client code. At the same time we have to run the spy server from the server-side. Login the spy- server, after successful login it will checks Admin ID and password and display the Home page. When the thread get initiated it will show the IP address of the client PC at the server side PC. Then we have to connect client IP address at server side. And the screenshots will be started of connected client PC's. If found any illegal activity at client-side, server can easily shutdown the client PC from server-side. Al the screen captures will be recorded and saved at server-side database. After the work completed you may stop the running code of spy-client as wel as spy-server.

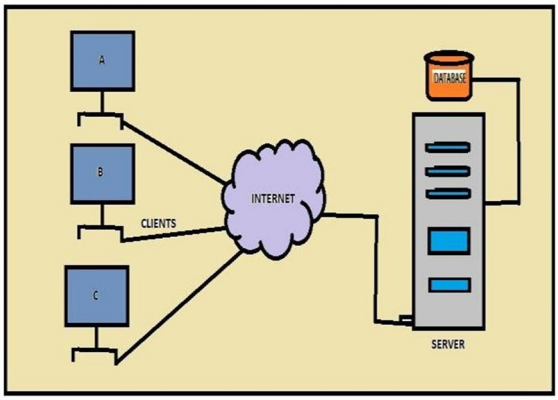


Fig.01. Block Diagram of spy-client and spy-server working in Single Network

In the above figure, A, B, C are the PC's i.e. Client or spy-client. All the PC's and server are connected in a same network. All the client PC's data will be monitored by the server. And accordingly, at the same time the monitored data will be stored at server- side database. The path of the storing data at proper location will be set and saved at the server-side PC. After every 0.2sec data will be captured.

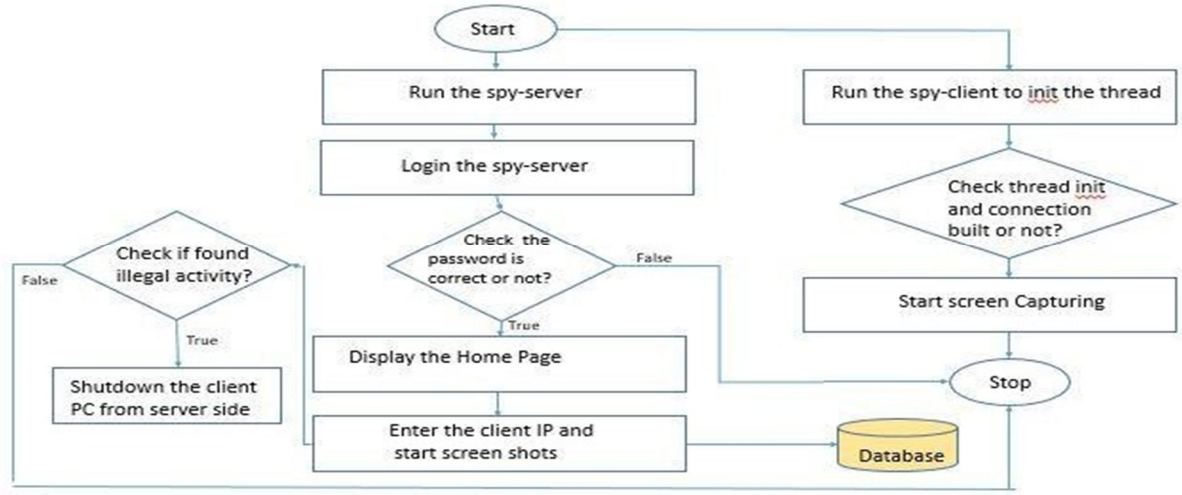


Fig.02. Data Flow Diagram of spy-client and spy-server working in Single Network

IV. FINDINGS & ANALYSIS

A. *Corcorrelation Between Distance and Time*

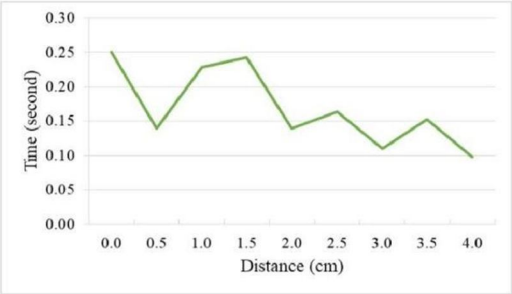


Fig.03. Correlation between distance and time

The testing of distance is also carried out to determine the effect of tapping distance on the serial number read time. Figure 2 shows the testing results of correlation between distance and time Based on the graph, it can be seen that the tapping distance does not affect the time required for reading the serial numbers. This is evidenced by the unstable time graph generated fromthe Test results. The average time taken by the card to read the serial number is less than 0.2 seconds.

B. *Testing Results*

Trial Number	Status
1	Success
2	Success
3	Success
4	Success
5	Success
6	Success
7	Success
8	Success
9	Success
10	Success
11	Success
12	Success
13	Success
14	Success
15	Success

The test results show that the reader can read the serial number properly. This is evidenced by the successful reading of the serial number 15 times. Thus, the percentage of successful reading the Serial number is 100%.

V. RESULTS

A. Testing of System Functionality

The testing of system functionality is used to determine the success of the features on the system. The Test results of system functionality are shown in below Table.

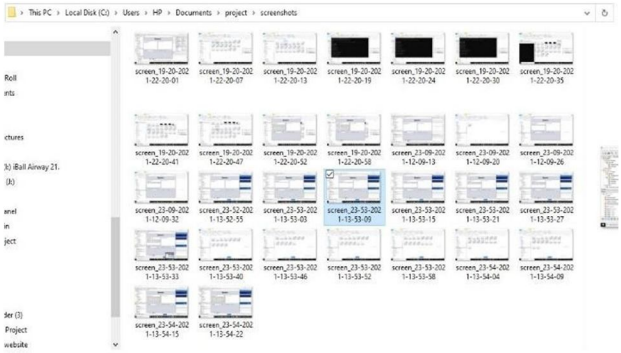
SR. NO.	TEST CASE	INPUT	ACTION	RESULT	STATUS
01	Server Login	Username and password	Enter valid username and password, then click login button. Enter invalid username and password, then click login button	Login success Login unsuccessful	Pass Fail
02	Network	Network connection	Check the spy-client and spy-server connected in same network or not. If connected then it will show the IP address If not connected then it will not show the IP address	Connection built successfully Connection not built	Pass Fail
03	Client IP address	IP address	First run the spy-client and init the thread. If thread not initiated	IP address shown. Thread initiated IP address not shown. Thread not initiated	Pass Fail
04	Start screen capturing from server side	Screen capture	Both spy server and spy client should be connected in the same network. Enter client IP and click on start screenshots. If correct client IP address If incorrect client IP address	Automatically capture the client screen. Invalid client IP	Pass Fail

After executing the code spy-client will capture image automatically. All the captured data wil be monitored by the server and the data will be stored at server side.

B. Spy-client

1) Client

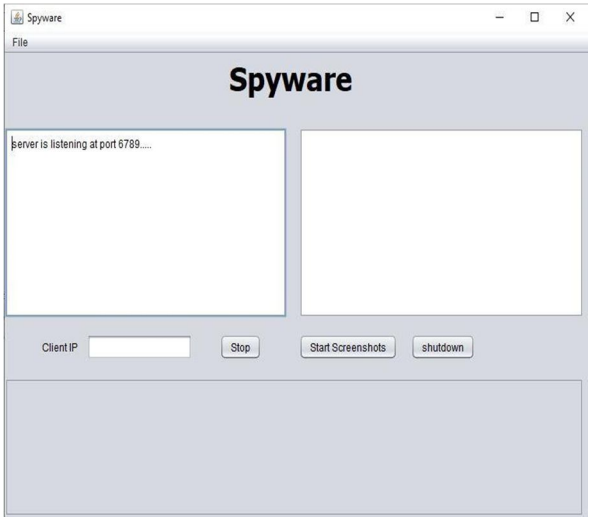
2) Capture Screenshots



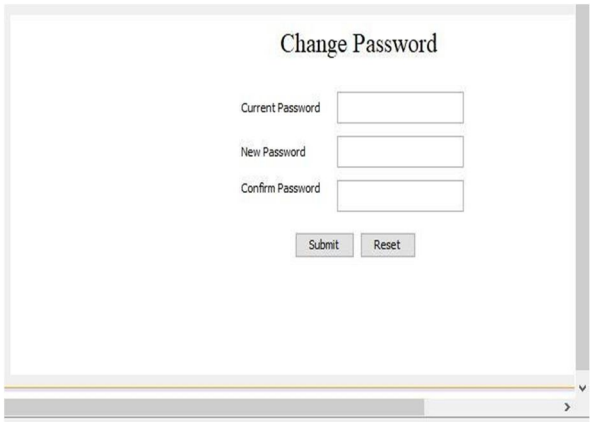
C. Spy- Server

1) Login

2) Home



3) Change Password



VI. DISCUSSION

Protecting information while ensuring availability and compliance with data privacy and security regulations are all done by this system. UAM goes beyond simply monitoring network activity. Including all system, data, application, and network actions that users take – such as their web browsing activity, whether users are accessing unauthorized or sensitive files, and more are all monitored automatically.

Main features in training User Activity Monitoring System(UAM) are:

A. Records user System Login Name

When a user logs in to the system (Windows, Terminal Session etc.) and enters his/her login name/password, computer monitoring software captures the login name. This information is used to identify who is using the computer. To catch the user's systemlogin name the software uses special system functions. Also computer monitoring software records system login and logout times to identify when the computer was used

.

B. Captures Applications Used

When a user runs various applications, computer monitoring software captures and records which applications are being run (How to monitor software use). This is done with the help of special systemfunctions.

Basically, computer monitoring collects lotsof data. To save disk space and minimize system resources use, computer monitoring software records used applications with a certain precision (for example, every 3 minutes).

C. Records Visited URLs

With the help of special system functions computer monitoring software monitors Internet use by recording website URLs

D. Stores Captured Information

All captured information is stored in a database. This is to generate reports and analyze computer use.

VII. CONCLUSION

Although user activity monitoring has its drawbacks considering the different circumstances, companies have the right to ensure that their employees are working productively, responsibly, and safely. When its implemented transparently and with sensitivity, UAM/Spyware tools can achieve their objectives without creating insecurities in the workplace. In any case, UAM/Spyware should beonly one component of a company's broader security efforts. As such, the data gathered from UAM/Spyware tools can and should be included in an organization's security analytics practice to help paint a full picture of its security posture.

From the college point of view now a day's Lab Assist take care of all the computers all alone. And also have to keep eye on each and every student while they are performing practical or any other college related work. Whether they are really doing assigned work or doing some suspicious activity. And it is extremely difficult to keep eye on each computer at the same time.

VIII. FUTURE SCOPE

Our project is easily extendable and can be improved by further for new and improved upgrades. New module can be easily added as it can be done an addition of a new package on click of a button. Our project has a big scope to do in the field of cyber security and protection of the company trade secrets and for the better work output of employees. As teachers can also get access to what students are doing on computer.

Though our project is matured enough but still there is still scope for betterment as it's always an open door. In this case we can also add some features to this software to make this software more reliable and robust. The project performs its intended functions with required precision, hence is very reliable and precise. The project is very flexible and any modification can be made to the existing system to suit changes that can take place in distant or immediate future. The online processing of the project is very simple following the existing method without any changes and suitable validation are provided for easy and correct access to user.

IX. ACKNOWLEDGMENT

We would like to express my deep sense of gratitude to Prof. Mr Virendra Yadav for sharing his expert views and continuous support as a guide. We also express our sincere thanks to Dr. S.A. Dhale, principal of Priyadarshini College of Engineering, Dr. Leena Patil, HOD of Computer Science and Engineering Department and Dr. Nilesh Shelke, Project In-charge for their kind co-operation, valuable guidance constant motivation, providing necessary infrastructure and all the facilities necessary for development of the project. We also thankful to al the faculty members and all non-teaching staff of the department & college for their co-operation throughout the project work. At last a special thanks to the researchers whose paper gave us the right direction to work.

REFERENCES

[1] The 1st Annual Technology, Applied Science and Engineering Conference IOP Conf. Series: Materials Science and Engineering 732 (2020) 012042 IOP Publishing doi:10.1088/1757- 899X/732/1/012042
[2] Hindawi Journal of Healthcare Engineering
[3] Volume 2019, Article ID 5674673, 13 pages https://doi.org/10.1155/2019/5674673
[4] 4th International Conference on Electronic Devices, Systems and Applications 2015 (ICEDSA) IOP Publishing IOP Conf. Series: Materials Science and Engineering 99 (2015) 012011 doi:10.1088/1757-899X/99/1/012011
[5] Research in INTERNATIONALJOURNALOF COMPUTER SCIENCES AND ENGINEERING June 2018 DOI: 10.26438/ijcse/v6i6.539542
[6] The 1st Annual Technology, Applied Science and Engineering Conference IOP Conf. Series: Materials Science and Engineering 732 (2020) 012042 IOP Publishing doi:10.1088/1757- 899X/732/1/012042

AUTHORS PROFILE

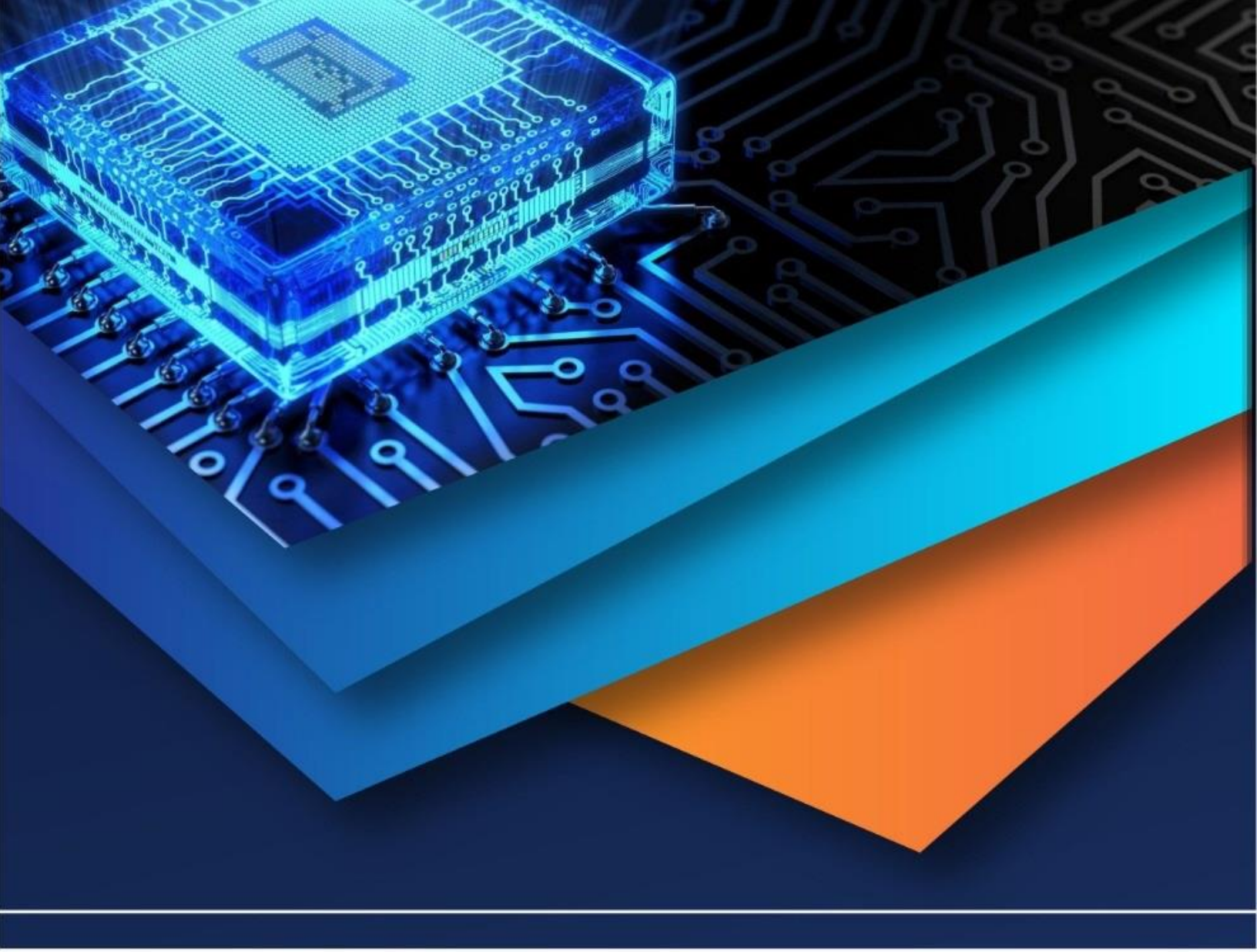
Sakshi Sanklecha is student at RTMNUUniversity, pursuing Engineering in Computer Science and Engineering, currently student at Priyadarshini College of Engineering, Nagpur, Maharashtra.

Darshit Deotale is student at RTMNU University, pursuing Engineering in Computer Science and Engineering, currently student at Priyadarshini College of Engineering, Nagpur, Maharashtra.

Jyoti Yadav is student at RTMNU University, pursuing Engineering in Computer Science and Engineering, currently student at Priyadarshini College of Engineering, Nagpur, Maharashtra.

Dipti Mishra is student at RTMNU University, pursuing Engineering in Computer Science and Engineering, currently student at Priyadarshini College of Engineering, Nagpur, Maharashtra.

Mr. Virendra Yadav is Assistant Professor at Department of Computer Science and Engineering in Priyadarshini College of Engineering, Nagpur, Maharashtra



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY